

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR ACCOUNT FOR TELEPHONE
NUMBER (423)763-3745 THAT IS
STORED AT PREMISES CONTROLLED
BY VERIZON WIRELESS

Case No. 1:20-mj- 124

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, John Barnett, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Cellco d.b.a. Verizon Wireless a wireless provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey, 07921. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Cellco d.b.a Verizon Wireless to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and have been since March 2015. I previously have approximately 15 years of local law enforcement experience. I am currently assigned to the ATF Chattanooga, Tennessee Field Office. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigators

Training Program. I am a graduate of the ATF National Academy's Special Agent Training Program. In the performance of my duties, I have conducted investigations for violations of state and federal laws, including drug trafficking, firearms trafficking, explosives crimes, and other violent crimes. Because of my training and experience as an ATF Special Agent, I am familiar with federal criminal laws relating to firearms, explosives, arson and illegal controlled substances.

3. Based upon my training, experience, and participation in investigations involving controlled substances, I know that when controlled substances are illegally used, manufactured, and trafficked, other supporting items and materials are usually present in addition to the controlled substances themselves. These supporting items commonly associated with the use of and trafficking of controlled substances include, but are not limited to, drug paraphernalia, scales, and packaging materials suitable for particular substance(s); records and notes (including computer and electronically stored) of controlled substance transactions; money (proceeds of or capital for controlled substance(s) transactions); firearms kept for protection; stolen property (often traded for controlled substances); electronic devices suitable for use in controlled substance transactions, recordings of such transactions, or electronic devices suitable for avoiding law enforcement.

4. It is also common for traffickers of these substances to use electronic communication devices such as cellular telephones, pagers, both numeric and two-way, and computers so that they can conduct their business at virtually any time without unnecessary delay. I know that these devices are usually found on or in very close proximity to these persons and that such electronic devices are capable of storing information such as phone numbers and/or coded messages which may lead to the identity of codefendants, coconspirators, and/or sources of supply. Cellular phones, phone records, device purchase agreements and other related documents related to the ownership are normally kept at their businesses, and/or places of operation. It is also

common for them keep their electronic communication devices and cellular telephones in close proximity to themselves, on their person, in their vehicles, or at their business or place of operation. Cellular telephones, in addition to being communication devices, are also storage devices for data. Data electronically stored inside cellular telephones include telephone numbers of associates, logs of the date and time that individual calls were made, voice and text messages from associates and photographs of the primary user, family members and associates, location information, internet browsing history, calendar entries, task lists, contact information, and other similar data. The data inside cellular telephones is evidence of such sales activity, demonstrates true ownership and control of the telephones, which can be registered to another person, and can be effectively used to corroborate the statements of witnesses. With the advent of “smart phones” all of the documents and information discussed within this section can be held on a smart phone in electronic format as well.

5. Based on my training and experience in conducting investigations involving controlled substances, I also know that drug dealers, while utilizing electronic communication devices to conduct their business, will often use “slang,” or “code words” when referring to their business activities. These code words may include reference to, but are not limited to, money, narcotics, other co-conspirators, and certain locations. Drug dealers use these code words in an attempt to conceal their illegal activities from law enforcement in an effort to avoid detection. I am also aware that specific slang and code words utilized by those trafficking in controlled substances may be influenced by various factors such as geographical area, cultural influences, and the type of controlled substance being trafficked.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code Section 846 and 841 have been committed by Julian ROLLINGS. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

9. The United States, including the Bureau of Alcohol, Tobacco, Firearms and Explosives, is conducting a criminal investigation of Julian Paul ROLLINGS and others regarding possible violations of Title 21, United States Code, Sections 841(a)(1), 846, and 843(b).

10. Since approximately July 9, 2020, the Bureau of Alcohol, Tobacco, Firearms and Explosives have been involved in an investigation involving Julian Paul ROLLINGS and others. Through this investigation, Julian Paul ROLLINGS was identified as a significant distributor and source of supply of methamphetamine in Tennessee.

11. On July 9, 2020, your Affiant conducted a proffer of a Federal inmate (hereafter referred to as Source 1, S1). During the proffer, S1 stated JP ROLLINGS aka Julian ROLLINGS is distributing approximately two-three kilos of methamphetamine. S1 stated ROLLINGS travels

to Atlanta, Georgia, every three days to pick up kilos of methamphetamine and transport the methamphetamine back to Chattanooga, Tennessee. S1 stated ROLLINGS carries two firearms with him during his trips to Atlanta. S1 stated ROLLINGS delivered approximately two kilos of methamphetamine to Adam AXMACHER in Sequatchie County, Tennessee. S1 stated ROLLINGS drives a grey Acura car or a yellow motorcycle to Atlanta to pick up the methamphetamine. S1 stated ROLLINGS usually pays a female to ride with him in an attempt to avoid law enforcement. Your Affiant conducted an independent investigation with this information and discovered that ROLLINGS does have a grey Acura registered with Tennessee Department of Motor Vehicles.

12. On July 16, 2020, your Affiant interviewed a Chattanooga Police Department confidential source (hereafter referred to as CS1) about narcotics trafficking in Chattanooga, Tennessee. CS1 stated it knows and has seen ROLLINGS transport kilos of methamphetamine from Atlanta to Chattanooga approximately every three days. CS1 identified a Tennessee driver's license picture of Julian ROLLINGS as "JP ROLLINGS". CS1 gave your Affiant the phone number for ROLLINGS as (423)763-3745. CS1 gave your Affiant the residence address of ROLLINGS in Chattanooga, Tennessee. CS1 stated ROLLINGS would utilize his mother's address in northwest Georgia to house money and methamphetamine. CS1 stated ROLLINGS usually drives a grey Acura TL with aftermarket rims to Atlanta and back to Chattanooga. ROLLINGS would usually stop at his mother's address in northwest Georgia on his way back to Chattanooga. ROLLINGS would then deliver kilos of methamphetamine to AXMACHER in Sequatchie County, Tennessee. Your Affiant conducted an independent investigation with this information and discovered through surveillance, Julian ROLLINGS lives at 203 Valley View Apartment 1, Red Bank, Tennessee. A grey Acura with a Tennessee tag registered to ROLLINGS

is frequently parked at the residence in addition to a yellow motorcycle (no tag). The phone number (423)763-3745 is registered through Cellco d.b.a. Verizon to Julian ROLLINGS.

13. On July 20, 2020, your Affiant received additional information from CS1 regarding ROLLINGS trafficking kilos of methamphetamine. CS1 stated ROLLINGS picked up three kilos of methamphetamine in Atlanta, Georgia and delivered three kilos of methamphetamine to Adam AXMACHER in Sequatchie County, Tennessee on July 18, 2020.

14. On July 22, 2020, your Affiant received additional information from CS1 regarding ROLLINGS trafficking kilos of methamphetamine. CS1 stated ROLLINGS used Millennial Taxi of Chattanooga, Tennessee to travel to Atlanta, Georgia. ROLLINGS then used the same Millennial taxi to transport the kilos of methamphetamine back to Chattanooga, Tennessee. CS1 stated Millennial taxi # 320 was used to transport the methamphetamine. CS1 stated ROLLINGS brother, Shannon ROLLINGS drives taxi's for Millennial taxi service. Your Affiant conducted an independent investigation with this information and discovered through Chattanooga Police Department, Millennial Taxi # 320 is registered to Shannon ROLLINGS.

15. On August 8, 2020, your Affiant received additional information from CS1. CS1 stated ROLLINGS co-conspirator Adam AXMACHER was arrested in Sequatchie County, Tennessee. ROLLINGS told CS1 law enforcement conducted a search warrant at AXMACHER's residence early that morning and arrested AXMACHER. Your Affiant conducted an independent investigation with this information and discovered the 12th Judicial Circuit Drug Task Force Agent Cody Smith had conducted an early search warrant at AXMACHER's residence on August 8, 2020. Agent Smith stated AXMACHER's residence is very far from the roadway and not visible. Agent Smith stated no press releases or formal charges had been released to the public at that time.

16. On August 6, 2020, a request to preserve text messages sent to and from (423)763-3745 was sent to Verizon Wireless by your Affiant. On August 9, 2020, your Affiant received notification back from Verizon Wireless acknowledging the preservation of text messages as reflected in *Verizon Wireless Case ID# 475231*.

17. In my training and experience, I have learned that Cellco d.b.a. Verizon Wireless is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for Verizon Wireless subscribers may be located on the computers of Verizon Wireless. Further, I am aware that computers located at Verizon Wireless contain information and other stored electronic communications belonging to unrelated third parties.

18. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of Verizon Wireless for weeks or months.

19. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by Verizon Wireless for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

20. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

21. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Station Equipment Identity (“IMEI”). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

22. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which “cell

towers” (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

23. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers’ full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers’ Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

24. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications.

25. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and

experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such “timeline” information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device’s owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Verizon Wireless to disclose to the government copies of the records and other information

(including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

27. Based on the forgoing, I request that the Court issue the proposed search warrant.

28. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

29. The government will execute this warrant by serving the warrant on Verizon Wireless. Because the warrant will be served on Verizon Wireless, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

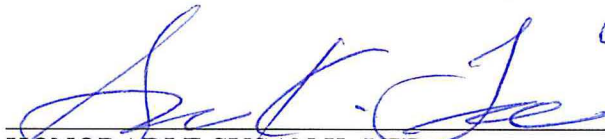
30. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed for 180 days. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



John Barnett
Special Agent
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Subscribed and sworn to before me on August 31, 2020



HONORABLE SUSAN K. LEE
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR ACCOUNT FOR TELEPHONE
NUMBER (423)763-3745 THAT IS STORED
AT PREMISES CONTROLLED BY
CELLCO D.B.A. VERIZON WIRELESS

Case No. 1:20-mj- 124

Filed Under Seal

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with CELLULAR ACCOUNT FOR
TELEPHONE NUMBER (423)763-3745 that is stored at premises owned, maintained,
controlled, or operated by Cellco d.b.a. Verizon Wireless, a wireless provider headquartered at
180 Washington Valley Road, Bedminster, New Jersey, 07921.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR ACCOUNT FOR
TELEPHONE NUMBER (423)763-3745
THAT IS STORED AT PREMISES
CONTROLLED BY CELLCO
D.B.A. VERIZON WIRELESS

Case No. 1:20-mj-124

Filed Under Seal

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Verizon Wireless

To the extent that the information described in Attachment A is within the possession, custody, or control of Verizon Wireless, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Verizon Wireless or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Verizon Wireless is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All voice mail, text, and multimedia messages **July 9, 2020 to Present** stored and presently contained in, or on behalf of the account or identifier;
- b. All existing printouts from original storage of all of the text messages described above;

c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from **July 9, 2020 to Present**;

d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message **July 9, 2020 to Present**

e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

f. Detailed billing records, showing all billable calls including outgoing digits, from **July 9, 2020 to Present**;

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from **July 9, 2020 to Present**

h. Incoming and outgoing telephone numbers, from **July 9, 2020 to Present**

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

j. All records pertaining to communications between Verizon Wireless and any person regarding the account or identifier, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 21, United States Code Sections 846 and 841 involving Julian ROLLINGS from **July 9, 2020 to Present** including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Evidence relating to the sale and distribution of controlled substances.
- b. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;
- c. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;
- d. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;
- e. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s)